UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

THE NEW YORK TIMES COMPANY, NICHOLAS CONFESSORE, and GABRIEL DANCE, Plaintiffs, -v- FEDERAL COMMUNICATIONS COMMISSION, Defendant.	18 Civ. 8607 (LGS)

SECOND DECLARATION OF ERIK SCHEIBERT

I, ERIK SCHEIBERT, pursuant to 28 U.S.C. § 1746, declare the following under penalty of perjury:

1. I currently serve as the Associate Chief Information Officer for Engineering and Chief Enterprise Architect within the Office of the Managing Director at the Federal Communications Commission ("FCC"). I explained my work history and expertise in my declaration of March 14, 2019, submitted at Docket No. 24 in *The New York Times Company, et al. v. Federal Communications Commission*, 18 Civ. 8607, currently pending in the United States District Court for the Southern District of New York. Again, I am the subject matter expert on the FCC's Electronic Comment Filing System ("ECFS"). This second declaration supplements the information provided in my March 14, 2019 declaration and is based on information and belief developed in the course of my duties at the FCC.

Users Do Not "Submit" Their IP Addresses or User-Agent Information

2. As I explained in paragraph 8 of my previous declaration, when an ECFS user submits comments, ECFS prompts users to provide their names and postal addresses. As I also explained at paragraph 16 of that declaration, the agency's computer servers automatically

generate server logs. Among the data automatically recorded in some of these logs is the ECFS user's IP address and the data in the "User-Agent" field. Again, the User-Agent field contains specific information about a user's computer system such as the operating system, operating system version, browser version, the browser platform, and the user's language settings. Unlike a user's name and mailing address, which a user directly and knowingly enters into a form when using ECFS to submit comments, users do not and cannot voluntarily "submit" their IP address or User-Agent information. That is, they do not knowingly type this information into a field and submit it. Many users are likely to be unaware that their computer is transmitting their IP address and User-Agent information to ECFS, and that the servers are collecting and retaining this information.

Even Dynamic IP Addresses Can Compromise A User's Privacy

3. Most consumer Internet users do not have permanent "static" IP addresses which remain the same indefinitely. Instead, they are assigned a "dynamic" IP address by their retail internet service provider ("ISP"). As the term "dynamic" indicates, a consumer's IP address can change, for example, when the ISP updates its servers or reconfigures its network devices or when it is otherwise expedient for the ISP to do so. Based on my experience as a network and security engineer, I believe there are at least three reasons that publicly disclosing the information that the Times requests from the FCC's logs could compromise a user's privacy, despite the fact that most individuals use dynamic IP addresses. First, some Internet users, including individual retail customers, pay to have a static address from their ISP to host their own Internet-available services such as email, web servers, or web-based cameras.

4. Second, even for users that have dynamic addresses, their IP address will remain unchanged for some time. Typically, an ISP assigns a user an address which is good for some

period of time (known as a lease), for example, three days. Prior to that lease expiring (usually at about 50% of the lease time), the user's router will request a lease renewal for that same IP address. Most of the time the ISP's servers will grant the request so the lease time is reset and the router keeps the same IP address. While most users with dynamic IP addresses who submitted comments to ECFS in 2017 will likely have different IP addresses today, it is far from certain that all those users will have new addresses or when those new addresses were obtained.

5. Third, even "outdated" IP address information can be useful to digital advertisers. As I described in my previous declaration at paragraph 36, digital advertisers specialize in tracking individuals across the Internet in order to form an extensive picture of consumer activity, demographic information, and so on. Such a company could make use of older IP addresses that are matched with names and addresses in ECFS. By combining this old IP address, linked to a person's identity, with other information about how IP address was used in the past, they can identify and learn more about a person's past online activity.

6. An IP address—whether it is static or dynamic, or whether it is assigned to an individual user or an organization—is formatted as a series of four values separated by periods. Although some ECFS users presumably have dynamic IP addresses while others have static ones, an ECFS server log does not distinguish between the two. Nor is there a way for a person reviewing that log to distinguish users who are individuals and those that are organizations, based solely on an IP address and User-Agent field. The IP addresses of individuals and organizations will look the same. A person reviewing server log entries therefore cannot distinguish between users that are individuals and users that are organizations, nor between users accessing ECFS with static IP addresses and users with dynamic IP addresses.

I declare under penalty of perjury that the foregoing is true and correct.

Dated: 5/2, 2019
Washington, D.C.

ERIK SCHEIBERT